

INTRODUCCIÓN A LA FORENSIA DIGITAL

- El análisis forense en un sistema informático es una ciencia moderna que permite reconstruir lo que ha sucedido en un sistema tras un incidente de seguridad.
- Puede determinar quién, desde dónde, cómo, cuándo y qué acciones ha llevado a cabo un usuario o intruso en los sistemas afectados por un evento de seguridad.

INTRODUCCIÓN A LA FORENSIA DIGITAL

- El análisis forense en un sistema informático es una ciencia moderna que permite reconstruir lo que ha sucedido en un sistema tras un incidente de seguridad.
- Puede determinar quién, desde dónde, cómo, cuándo y qué acciones ha llevado a cabo un usuario o intruso en los sistemas afectados por un evento de seguridad.

IFD: EL PROCESO FORENSE

- La naturaleza de la evidencia digital es tal que esta posee desafíos para su admisibilidad en procesos legales.
- Para hacer frente a estos desafíos, hay que seguir procesos forenses adecuados.
- Estos procesos se componen básicamente de 4 fases:
 1. Recolección
 2. Examinación/Extracción.
 3. Análisis.
 4. Reporte.

¿QUÉ OCURRE EN EL MUNDO REAL?

For anyone who is interested about the poor security practices in use at Globant.com. i will expose the admin credentials for ALL there devops platforms below.

<https://confluence.globant.com/>

<https://confluence.corp.globant.com/> (massive, over 3000 spaces of customer documents)

admin

oighiegh

<https://crucible.globant.com/>

<https://crucible.corp.globant.com/>

admin

aiyiushe

<https://jira.globant.com/>

<https://jira.corp.globant.com/>

admin

ohgheibi

admin2

ohgheibi

<https://github.globant.com/>

<https://github.corp.globant.com/>

syed.aleem

New123456789!!!

|

¿QUÉ OCURRE EN EL MUNDO REAL? A QUIÉN SE PERSIGUE?

We recruit employees/insider at the following!!!!

- Any company providing Telecommunications (Claro, Telefonica, ATT, and other similar)
- Large software/gaming corporations (Microsoft, Apple, EA, IBM, and other similar)
- Callcenter/BPM (Atento, Teleperformance, and other similar)
- Server hosts (OVH, Locaweb, and other similar)

TO NOTE: WE ARE NOT LOOKING FOR DATA, WE ARE LOOKING FOR THE EMPLOYEE TO PROVIDE US A VPN OR CITRIX TO THE NETWORK, or some anydesk

If you are not sure if you are needed then send a DM and we will respond!!!!

If you are not a employee here but have access such as VPN or VDI then we are still interested!!

You will be paid if you would like. Contact us to discuss that

[@lapsusjobs](#) 51,3K edited 17:36

 849 Comments >

COLONIAL PIPELINE 2021

- El ciberataque de Colonial Pipeline tuvo lugar entre el jueves 6 de mayo y el viernes 7 de mayo de 2021
- Cuando Colonial Pipeline sufrió un ataque de malware que los obligó a cerrar su sistema.
 1. El ataque detuvo todas las operaciones del oleoducto.
 2. Colonial Pipeline dijo que el ataque afectó a algunos de sus sistemas de información. El presidente Joe Biden declaró el estado de emergencia el domingo 9 de mayo.
 3. Fue «lo que se cree que es el mayor ciberataque exitoso a la infraestructura petrolera en la historia del país» y una fuente le dijo que el ataque fue llevado a cabo por una empresa criminal de ransomware llamada DarkSide, y no por un gobierno extranjero.
 4. Se cree que el mismo grupo robó 100 gigabytes de datos de los servidores de la empresa el día antes del ataque de malware.

COLONIAL PIPELINE 2021



COLONIAL PIPELINE 2021

Petroleum product supply overview U.S. Gulf Coast and East Coast regions

eria



Source: U.S. Energy Information Administration, *East Coast and Gulf Coast Transportation Fuels Markets*
Note: Map updated to reflect changes in U.S. refineries since initial report.

A QUIÉN PERSIGUEN?

The New York Times

The F.B.I. confirms that DarkSide, a ransomware group, was behind the hack of a major U.S. pipeline.

A deputy national security adviser said that the government believed DarkSide was “a criminal actor” but was looking for any ties to nation-states.



DarkSide hackers say the Colonial Pipeline cyber attack was only about the money — not politics

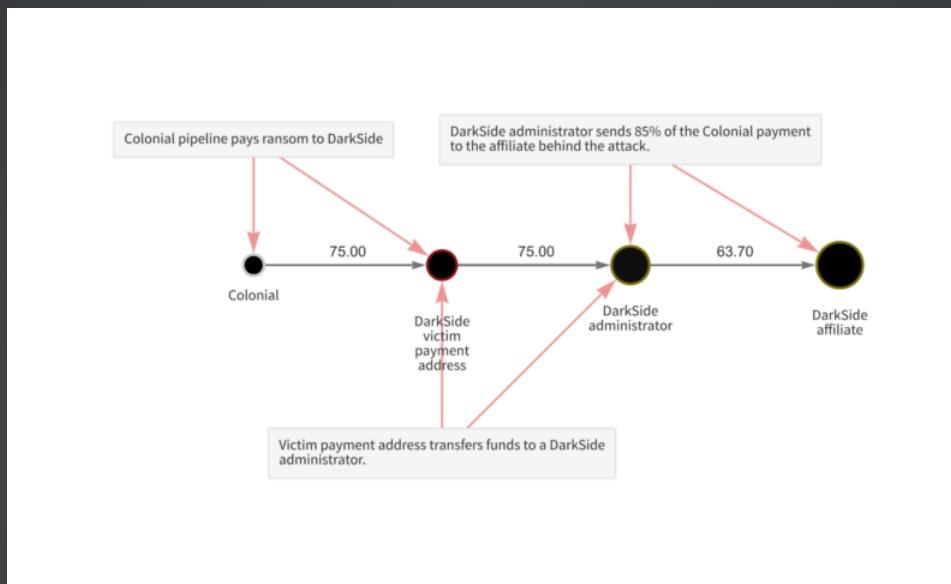
CRONOLOGÍA DEL ATAQUE Y LA RESPUESTA

- Mayo 2021: Colonial Pipeline sufre un ataque de ransomware de DarkSide.
- La empresa paga 75 BTC (~4.4 millones USD en ese momento) a los atacantes.
- El ataque causa interrupción del suministro de combustible, lo que genera escasez y pánico en varias regiones de EE. UU.
- Seis días después, Colonial reanuda operaciones.
- Un mes después: el Departamento de Justicia (DoJ) anuncia la recuperación de \$2.3 millones en BTC (parte del pago original).
- URL

MODELO RANSOMWARE-AS-A-SERVICE (RAAS)

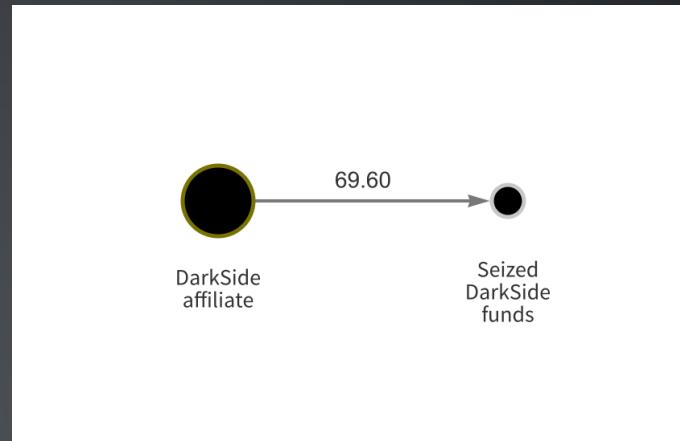
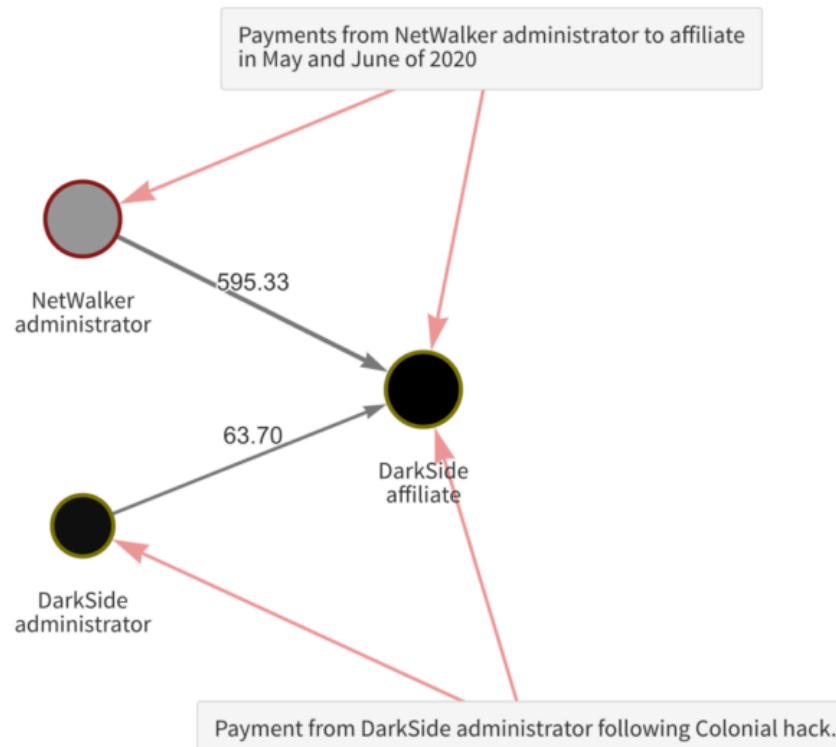
- DarkSide provee la infraestructura y el malware a “afiliados”.
- Los afiliados ejecutan el ataque en la víctima.
- Los administradores se quedan con una comisión del rescate.
- Ventaja para los atacantes: escalabilidad y anonimato en la distribución de funciones.
- Desventaja para las víctimas: aumenta el número de grupos capaces de lanzar ataques complejos.

LA FORENSIA - FOLLOW THE MONEY



- Colonial → Dirección de los atacantes: 75 BTC.
- Atacantes → Administradores de DarkSide: Los administradores retienen un 15% (~11.3 BTC).
- Administradores → Afiliado (ejecutor del ataque): 63.7 BTC ($\approx 85\%$).
- FBI logra rastrear y confiscar fondos del afiliado el 28 de mayo de 2021.

LA FORENSIA - FOLLOW THE MONEY



EL RASTRO -> RECUPERANDO 63.7/75 BITCOINS

- An affidavit filed on Monday said the FBI was in possession of a private key to unlock a bitcoin wallet that had received most of the funds. It was unclear how the FBI gained access to the key.

EL FBI ARRESTÓ A UNA CONTRATISTA DE LA NSA (2017)

- El FBI arrestó a una contratista de la NSA de 25 años por filtrar información al diario The Intercept sobre los ataques rusos a las empresas de máquinas de votación



EL FBI ARRESTÓ A UNA CONTRATISTA DE LA NSA

- La agarraron mediante una forensia rara
 - The Intercept envía el documento a la NSA para verificar y darles lugar a comentarios: **tengo esto! que tenes para decir?**
 - El documento resulta ser un scanning de una impresión
 - Se supone que hizo esto para evitar metadatos del archivo

EL FBI ARRESTÓ A UNA CONTRATISTA DE LA NSA

- Pero, por desgracia para ella, parece que no era consciente del hecho de que:
 - la mayoría de las nuevas impresoras imprimen puntos amarillos casi invisibles que registran exactamente cuándo y dónde se imprime cualquier documento

EL FBI ARRESTÓ A UNA CONTRATISTA DE LA NSA

- Información en ese documento permite saber:
 - la impresora que lo imprimió
 - el horario
 - Cruzándolo con los datos de los usuarios en los equipos
- Link: <http://thehackernews.com/2017/06/nsa-russian-hacking-leak.html>

MANCHAS INVISIBLES

The screenshot shows a web browser window titled "EFF: DocuColor Tracking Dot". The URL is [https://w2.eff.org/Privacy/printers/docucolor...](https://w2.eff.org/Privacy/printers/docucolor/). The page displays a grid of yellow dots representing a tracking pattern. To the left of the grid, there are numerical columns labeled 1 through 15 and rows labeled 1 through 7. A column labeled "col parity" has values 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, and 15. The grid itself has 15 columns and 7 rows. Below the grid, there are two buttons: "Clear" and "Submit". To the right of the grid, the text "DocuColor pattern interpretation" is displayed, followed by "This is an interpretation of the following dot pattern:" and a binary string representation of the pattern. The binary string is:

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	1	1	1	1	1	1	1	1	1	1	1	1	1	1
4	1	1	1	1	1	1	1	1	1	1	1	1	1	1
5	1	1	1	1	1	1	1	1	1	1	1	1	1	1
6	1	1	1	1	1	1	1	1	1	1	1	1	1	1
7	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Below this, a note states: "This interpretation is based on reverse engineering, and may current for every DocuColor model version. Xerox Corpora with this program, and does not warrant its correctness." Further down, it says "Row and column parity verified correctly.", "Printer serial number: 535218 [or 29535218]", "Date: May 9, 2017", and "Time: 06:20".

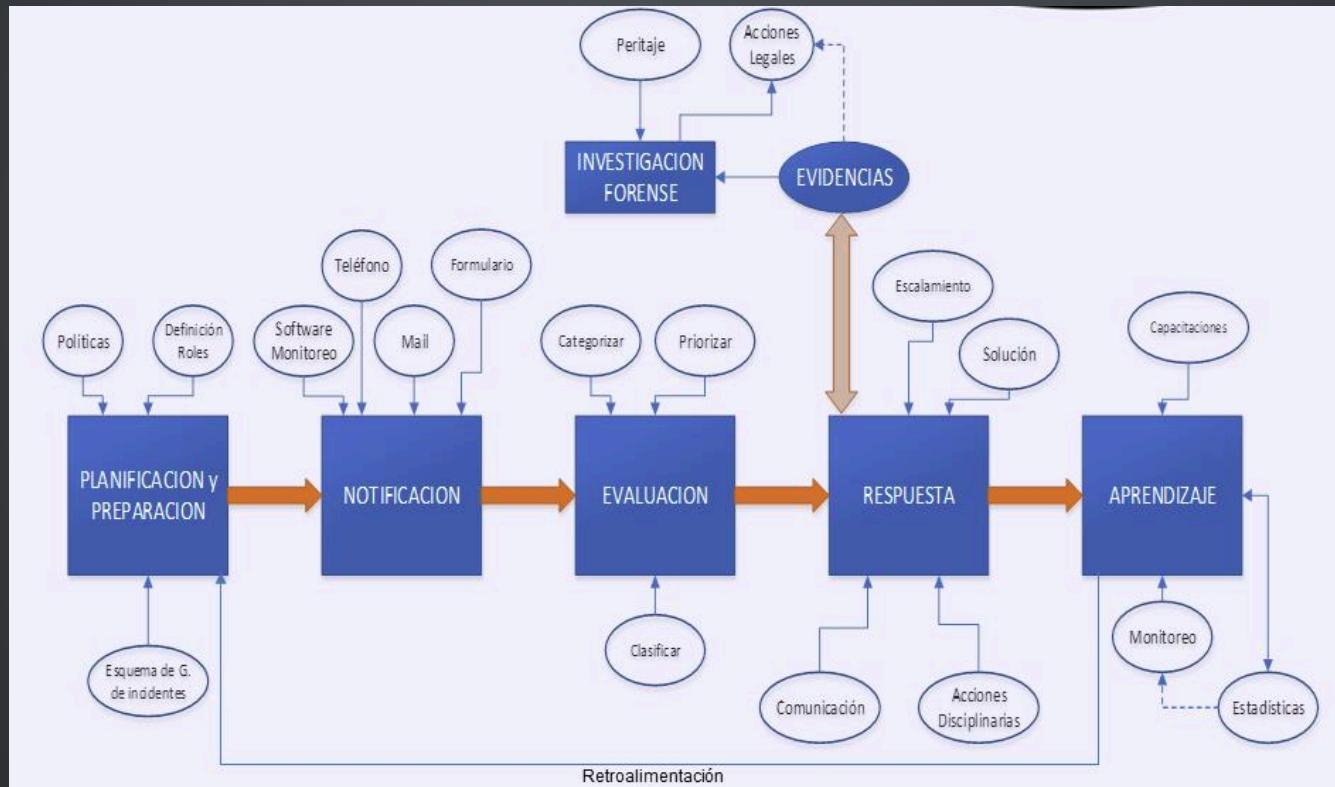
- "The document leaked by the Intercept was from a printer with model number 54, serial number 29535218. The document was printed on May 9, 2017, at 6:20. The NSA almost certainly has a record of who used the printer at that time."

RESULTADO DE LA PERICIA



GESTIÓN DE INCIDENTES

- Proceso para planificar, detectar, informar, evaluar, responder, tratar y aprender de los incidentes de seguridad.



UN EJEMPLO DE UN MAL PROCESO

El Renaper detectó el uso indebido de una clave otorgada a un organismo público y formalizó una denuncia penal

Compartir en
redes sociales



Publicado el miércoles 13 de octubre de 2021

El Registro Nacional de las Personas (Renaper) formalizó ayer una denuncia penal ante el Juzgado en lo Criminal y Correccional Federal N° 11 Secretaría N° 22 tras detectar que, mediante el uso de claves otorgadas a organismos públicos, en este caso el Ministerio de Salud, se filtraron imágenes como perteneciente a trámites personales realizados en el Renaper. Desde el organismo dependiente del Ministerio del Interior se confirmó que se trató de un uso indebido de usuario o robo de la clave del mismo, y que la base de datos no sufrió vulneración o filtración alguna de datos.

El sábado 9 de octubre el Renaper tomó conocimiento de que un usuario de Twitter identificado con el nombre de @aniballeaks -cuenta que fue denunciada y que actualmente se encuentra suspendida- había publicado en dicha red social las imágenes de 44 individuos, entre los cuales se encontraban funcionarios y personajes públicos de conocimiento en general.



Publicación oficial

UN EJEMPLO DE UN MAL PROCESO - LA POSTA

- Se filtra en RAIDFORUMS (un foro sospechoso.....)
- 65000 registros disponibles como muestra de concepto de un total de 45.387.114 supuestos en la base completa
- Los campos que ofrecen son: indice, id, idtramiteprincipal, idtramatetarjetareimpresa, ejemplar, vencimiento, emision, apellido, nombres, fechaNacimiento, cuil, calle, numero, piso, departamento, cpostal, barrio, monoblock, ciudad, municipio, provincia, pais, mensaf, foto, sexo, numeroDocumento, idciudadano.

UN EJEMPLO DE UN MAL PROCESO - LA POSTA [LINK](#)

SELLING Argentina Citizens Full Database 45M

by cfk - October 10, 2021 at 09:29 PM

Pages (4): 1 2 3 4 Next »

October 10, 2021 at 09:29 PM This post was last modified: 1 hour ago by cfk. Edited 4 times in total.

#1

★ cfk



V.I.P User

VIP

Posts 14
Threads 4
Joined Sep 2021
Reputation 20



Database obtained from the National Population Registry of Argentina (RENAPER).

Includes photo in base64, names, lastnames, addresses, gender, deceased or not, ID processing number, ID card information, code located on the back of the card (three lines barcode) calculated by an algorithm and all the necessary data to create a false identity card.

Total records in database: 45.387.114

Example with ID of the president Alberto Fernandez:

```
[idtramiteprincipal] => 102677495      # Processing number  
  
[idtramitetarjetareimpresa] => 102677495      # Processing number in card  
  
[ejemplar] => A      # Copy  
  
[vencimiento] => 23/03/2027      # Expiration date
```

60.000 sample records:

Quote:

https://anonfiles.com/nc91BdP7uf/renaper_samples_json

The database in SQL or JSON format.

Price is 0.29 BTC or XMR too.

For business contact me via PM or jabber: tango11@jabber.no

MIENTRAS TANTO UN BUEN PROCESO DEBERÍA TERMINAR ASÍ

The screenshot shows a web browser window with the URL raidothreads.com in the address bar. The page content is a standard "Domain Seized" template. At the top, it says "THIS DOMAIN HAS BEEN SEIZED". Below that, it identifies the domain as "The domain for RAIDFORUMS.COM". The main text explains that the domain was seized by multiple law enforcement agencies: the Federal Bureau of Investigation, the United States Secret Service, and the Department of Justice, in accordance with a seizure warrant issued pursuant to 18 U.S.C. §§ 981, 982, inter alia, by the United States District Court for the Eastern District of Virginia as part of law enforcement action taken in parallel with Europol's Joint Cybercrime Action Task Force, the United Kingdom's National Crime Agency, the Swedish Police Authority, the Romanian National Police, the Internal Revenue Service Criminal Investigation and other international law enforcement partners.

Logos of the seized entities are displayed at the bottom:

- Department of Justice
- Federal Bureau of Investigation
- United States Secret Service
- IRS:CI
- Polisen Swedish Police
- EUROPOL
- NCA National Crime Agency
- Romanian National Police
- Policía Judiciaria

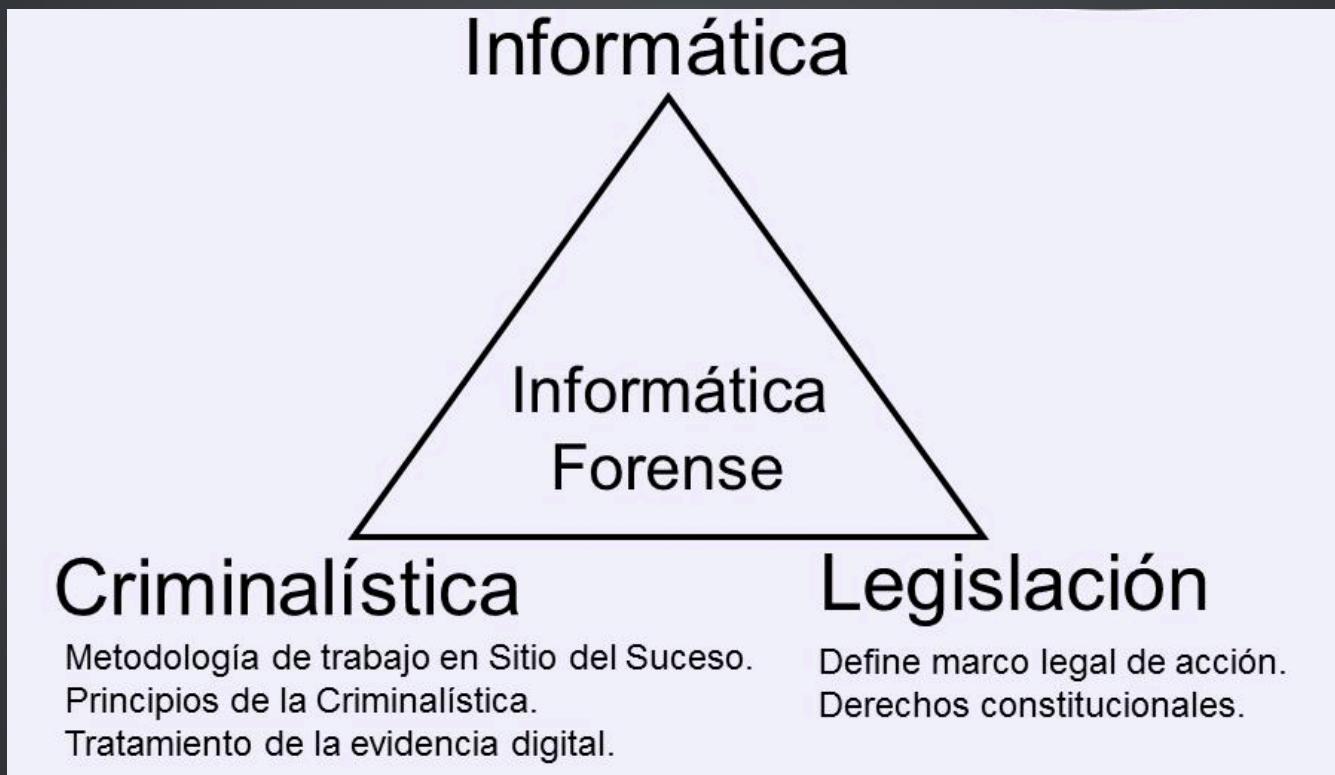
INTRODUCCIÓN A LA FORENSIA DIGITAL - RECAPITULANDO ENTONES

- El análisis forense en un sistema informático es una ciencia moderna que permite reconstruir lo que ha sucedido en un sistema tras un incidente de seguridad.
- Puede determinar quién, desde dónde, cómo, cuándo y qué acciones ha llevado a cabo un intruso en los sistemas afectados por un incidente de seguridad.

IFD: CONCEPTOS

- Informática forense
 - Área de la informática que es auxiliar de la justicia en los ámbitos legales correspondientes a la informática.
 - Según el FBI, es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y almacenados en un medio computacional.

IFD: CONCEPTOS



IFD: CONCEPTOS

- Indicio
 - Todo elemento perceptible que permite imaginar la existencia de una circunstancia determinada vinculada al suceso investigado (pista)
 - Su posterior análisis puede servir para encontrar evidencias.
 - Ejemplo:
 - La desaparición de un objeto que debería estar presente o la recolocación de mobiliario en la escena pueden ser indicios. Se trata de elementos que permiten apuntar en una determinada dirección, pero el cómo y hacia adonde apunten reviste cierta subjetividad por parte de los investigadores

IFD: CONCEPTOS

- Evidencia
 - Cuando un indicio permite establecer una **relación** con otro elemento que se encuentra vinculado al suceso investigado, se transforma en evidencia
 - Cuando la evidencia es aceptada por la autoridad judicial, pasa a ser prueba de un determinado hecho
 - Ejemplo:
 - Huellas dactilares en un objeto robado o restos de sangre sobre una persona u objeto

IFD: CONCEPTOS

- Prueba
 - Argumento que demuestra la existencia o no de los hechos controvertidos y conducentes. Se utiliza la evidencia para demostrar el hecho que se presume
- Medios de prueba
 - Los medios que autoriza y reconoce por efficaces la ley
- Lugar del hecho (escena del crimen)
 - Lugar donde ha ocurrido un hecho que es necesario investigar, ya sea desde el punto de vista policial o judicial
 - Debe ser analizado en búsqueda de señales, rastros o indicios

IFD: ASPECTOS INVOLUCRADOS EN LA INFORMÁTICA FORENSE

- Informática: conocimientos esenciales en la materia
- Criminalística: lugar del hecho y tratamiento de la evidencia digital
- Legislación: conocer el proceso judicial que interviene o podría intervenir

IFD: EVIDENCIA DIGITAL

- La evidencia digital es información y datos de valor investigativo que es guardada en o transmitida por un dispositivo electrónico.
 - Suele ser latente en el mismo sentido en que las huellas digitales y el ADN son latentes.
 - Puede trascender fronteras con facilidad y rapidez, no es lo mismo, por ejemplo llevar cajas con documentos en barco de acá a China que enviar un archivo vía Dropbox.
 - Es frágil y puede ser fácilmente alterada, dañada o destruida, por examinación o manejo inapropiado.
 - En algunos casos puede llegar a ser time-sensitive.

IFD: EVIDENCIA DIGITAL

- Cuando se trabaja con evidencia digital hay principios de forensia general y procedural que deben ser aplicados:
 - Las acciones tomadas para recolectar y asegurar la evidencia digital no deben cambiarla ni modificarla en ningún sentido. (Hashing y Cadena de custodia)
 - Las personas que dirijan la examinación de la evidencia digital deben estar entrenadas en el campo.
 - La actividad relacionada debe ser documentada en su totalidad, ya sea la incautación, la examinación, el almacenamiento o la transferencia de la evidencia digital.

IFD: MOTIVOS PARA INVESTIGAR UN INCIDENTE

- Si bien como mencionamos antes la finalidad es reconstruir lo sucedido hay distintos motivos que lo pueden justificar y dependiendo el motivo son los recaudos que hay tomar:
 - **Legales:** cuando el requerimiento es requerido por un proceso de algún tipo, como un proceso judicial, que requiere la conservación de la validez de las evidencias.
 - **No legal:** cuando la necesidad de averiguar que ocurrió obedece a motivos no legales, como ser necesidad de recuperar un servicio dañado o conocer el alcance de un malware.
- El ámbito puede ser privado y público.

IFD: LA CADENA DE CUSTODIA

- Es uno de los protocolos de actuación que ha de seguirse con respecto a una prueba durante su período de vida o de validez, desde que ésta se consigue o genera, hasta que se destruye, o deja de ser necesaria.
- Este protocolo debe controlar dónde y cómo se ha obtenido la prueba, qué se ha hecho con ella -y cuándo-, quién ha tenido acceso a la misma, dónde se encuentra ésta en todo momento y quién la tiene y, en caso de su destrucción –por la causa que sea-, cómo se ha destruido, cuándo, quién, dónde y porqué se ha destruido.

IFD: LA CADENA DE CUSTODIA

LA CADENA DE CUSTODIA

- Se utiliza para documentar información vital sobre la evidencia adquirida.
- La documentación esencial para la evidencia digital sería:
 - Fecha y hora de la adquisición.
 - De donde se ha extraído la información (serial y modelo del dispositivo).
 - ¿Qué método ha sido utilizado para extraer la imagen?
 - Hash de la evidencia y cual función fue utilizada para generarla (md5,sha1,etc).
 - Personas involucradas en la transferencia.

IFD: LA CADENA DE CUSTODIA

- La cadena debe cumplirse para que la evidencia sea válida.
- Debe ser actualizada cada vez que la evidencia es transferida.
- Toda copia de la evidencia debe tener un formulario de "copia de evidencia"

IFD: EL PROCESO FORENSE

- La naturaleza de la evidencia digital es tal que esta posee desafíos para su admisibilidad en procesos legales.
- Para hacer frente a estos desafíos, hay que seguir procesos forenses adecuados.
- Estos procesos se componen básicamente de 4 fases:
 1. Recolección
 2. Examinación/Extracción.
 3. Análisis.
 4. Reporte.